REMARKS

The final Office Action mailed on January 22, 2009 (Paper No. 20100116) has been carefully considered.

The specification is being amended to improve its form, claim 5 is being amended, and new claims 9-13 are being added. Thus, claims 5-13 are pending in the application.

A Request for Continued Examination (RCE), including a request for entry of this Amendment after Final, is being filed concurrently herewith. Therefore, this Amendment after Final should be entered.

Claims 5-8 are rejected under 35 U.S.C. 103 for alleged unpatentability over Sasmazel, European Patent Application No. 1328101A2 in view of Zeidler, U.S. Patent No. 4,578,530. For the reasons stated below, it is submitted that the invention as claimed is distinguishable from the cited reference so as to preclude rejection under 35 U.S.C. 103.

Amendment of Independent Claim 5

Independent claim 5 is being amended in a minor manner.

Specifically, the word "allocated" on line 10 of the claim is being changed to "assigned" so as to compensate for slightly inaccurate translation of the original application into English, and so as to more accurately describe the relationship between the coding and decoding keys and the information transmitting terminal device.

In addition, the word "the" on line 17 of the claim is being replaced by the word "individual" so as to more accurately describe that the "coding keys" belong to "individual information transmitting devices".

Finally, on line 24 of the claim, the word "which" is being inserted to improve grammatical form.

Therefore, as stated above, these minor amendments are for the purpose of improving the form and accuracy of the claim.

Addition of Dependent Claims 9-13

New dependent claims 9-13 recite features and functions of the invention which result from the structure of the present invention, as recited in independent claim 5, and as described in the specification of the present application. See also the discussion in the section entitled "Additional Arguments" contained on pages 21-25 of this Amendment after Final.

Rejection under 35 U.S.C. 103

It should first be noted that the secondary reference cited against this application, Zeidler '530, was cited in the International Search Report relative to the corresponding international application, but was designated as falling in Category A, that is, a "document defining the general state of the art which is not considered to be of particular relevance"

(quoting from page 1 of the International Search Report). A copy of the International Search Report was filed with this application in the Patent and Trademark Office on September 1, 2006.

Furthermore, a claim corresponding to independent claim 5 was presented to the International Preliminary Examining Authority (IPEA) in order to overcome a rejection, and the claim corresponding to independent claim 5 was found by the European Patent Office (EPO) to distinguish the invention from the prior art, including the two references now cited in the present Office Action, was allowed by the EPO, and was validated in over twenty (20) European countries.

Discussion of the Cited References

The cited reference, Sasmazel '101, presents a set of equipment which realizes coded information transfer with a combination of centralized communication networks similar to the traditional telephone system and the TAN number system known in the financial community. The disadvantage of the method and apparatus of Sasmazel '101 is that it uses a single-key algorithm for the coding of communications, and it stores all of the keys in a single place in a main element of the system, the call complex 102 of Figure 1 of the reference. Furthermore, all of the communication occurring in the system travels through the call complex 102. As a result, the system of Sasmazel '101 is vulnerable because, if the call complex 102 is controlled by an unauthorized person, or if the keys stored in the call

complex 102 are illegally possessed, all of the communications taking place in the network can be decoded by unauthorized persons. Thus, the call complex 102 of Sasmazel '101can become a primary target for access attacks.

A further disadvantage of the method and apparatus of Sasmazel '101 is that it is the call complex 102 itself that initiates communication in order to establish calls with called end terminals. This makes the call complex 102 vulnerable to well-known hacker techniques. Another serious security flaw in the method and apparatus of Sasmazel '101 is that all of the section keys required for the interpretation of communications are transmitted over the communication channel of the call complex 102 through a set network point, even though coded. The section keys also pass through the network during the call establishment process. This characteristic also creates an opportunity for potential attack. In addition, the method and apparatus of Sasmazel '101 uses the same section key for both directions of communication (see SKLST[n] of Figure 3 of the reference) so that acquisition of one key makes it possible to eavesdrop on the entire communication.

A further disadvantage of the method and apparatus of Sasmazel '101 is that, since all communication is carried out through the call complex 102, the data transfer capacity of the call complex is continually burdened in proportion to the number of communications taking place at any specific point in time. As a result of the above security deficiencies, the method and apparatus of Sasmazel '101 are not suitable for creating a secure, general-purpose Internet Protocol (IP)-based network with system-level protection. In contrast, the

disadvantages and deficiencies of the method and apparatus of Sasmazel '101, including its security flaws, do not occur in the present invention.

Specifically, in the present invention, only asymmetric keys are used for securing the system. The keys required for the decoding and interpretation of communications never pass through the communication network while the system is operating, and the decoding keys never leave the end terminals or the central traffic coordination unit. Moreover, these keys cannot be found together at any single point in the system so that, in accordance with the invention, the set of devices has in it no point which can be broken into. As a result, it is not possible for all communications in the system to be illegally decoded. In addition, even if the central traffic coordination unit or data stored therein were to become illegally possessed, it would still be impossible to decode communications taking place in the system.

Furthermore, in the present invention, the central traffic coordination unit is essential and unavoidable for the construction of the communication channel between the end terminals, but the constructed communication channel does not pass through the central traffic coordination unit so that communication between the end terminals takes place directly between the end terminals. Accordingly, simultaneous instances of communication only use the capacity of the central traffic coordination unit when constructing the communication channel, but do not use it when the communication is taking place.

In addition, in accordance with the present invention, there is no single network point through which all communication channels pass. A further significant difference between the claimed invention and the prior art is that, in the invention, the central traffic coordination unit never initiates communication so that the central traffic coordination unit is protected against attacks that use communication initiation.

Due to these important and basic differences between the invention and the prior art, it can be concluded that the locations and "movement" of the code keys employed in the invention could not be set up in the apparatus and method disclosed in Sasmazel '101, as well as in other prior apparatuses and methods. This is due to the fact that the structure of the invention, the location of the code keys, and the movement thereof differ from those of known systems, resulting in achievement of an inventive step not found in prior systems.

It should be noted that the above arguments were presented to the International Preliminary Examining Authority (IPEA) in order to overcome a rejection of the corresponding international application based on the same reference (Sasmazel '101), and that the claims of the corresponding international application recite the same subject matter as, and are virtually identical to, the claims pending in the present application. Moreover, it should also be noted that the international claims were accepted by the European Patent Office (EPO) and that, as a result, a European patent was granted and was validated in more than twenty (20) European countries. Therefore, for the same reasons that the claims of the

international application were allowed and were validated throughout Europe, the present U.S. claims should also be allowed.

Discussion of Cited Prior Art

However, there are additional reasons for distinguishing the invention claimed herein from the cited prior art. Specifically, on page 2 of the final Office Action, the Examiner alleges that, in Sasmazel '101, each transmitting terminal device (end unit 110 of Figure 1) includes a receiver partial unit and a storage partial unit, the Examiner citing column 5, lines 35-45 and column 8, lines 23-32 of Sasmazel '101 (see paragraph 3, lines 1-8 on page 2 of the final Office Action). However, such is not the case because column 5, lines 35-45 of Sasmazel '101 only discloses a memory 202 contained in the call complex 102 which, according to the Examiner's analysis, corresponds to the claimed central traffic coordination unit, while column 8, lines 23-32 does not mention any receiver partial unit or storage partial unit at all. Thus, Sasmazel '101 does not disclose or suggest a receiver partial unit and/or a storage partial unit disposed in a transmitting terminal device, as recited in independent claim 5. This is admitted on page 5 of the final Office Action (see page 5, lines 6-11 of the final Office Action).

In the latter regard, on page 5 of the final Office Action, the Examiner alleges that these features are well known in the art, and cites Figure 3 of Zeidler '530 as allegedly disclosing a receiver partial unit and a storage partial unit. However, the Examiner does not

cite any element in Figure 3 of the reference as corresponding to the receiver partial unit or the storage partial unit recited in independent claim 5 of this application (see page 5, lines 2-15 of the final Office Action). In fact, the description of Figure 3 appearing at column 7, lines 28-30 of Zeidler '530 states that Figure 3 of the reference is an optional block diagram representation of the manner in which a user initiated transaction request is initially processed by the transaction terminal. Thus, there would be no need for a receiver partial unit in Figure 3 since the arrangement disclosed therein is used only for the purpose of preparing transmissions.

In fact, a review of the detailed description of Figure 3 (appearing at column 10, line 67-column 12, line 68 of Zeidler '530) does not reveal any mention of a receiver partial unit or a storage partial unit with the functions recited in independent claim 5 of the present application.

Finally, in the paragraph bridging pages 7 and 8 of the final Office Action, the Examiner counter-argues that "Sasmazel discloses in paragraph 34 that each unit terminal comprises memory (e.g., storage) and one or more interfaces (e.g., receiver partial unit)" (quoting from the sentence bridging pages 7 and 8 of the final Office Action). However, whereas paragraph 34 of Sasmazel '101 mentions call complex 102, there is no mention whatsoever of a memory or interfaces, as alleged by the Examiner.

On page 8 of the final Office Action, the Examiner further argues that "the teaching of Zeidler provides storage for key data. Refer to fig. 3, figure item 34" (quoting from age 8,

lines 1-2 of the final Office Action). However, that does not constitute a disclosure of a receiver partial unit or storage partial unit as recited in independent claim 5.

At page 2, last two lines of the final Office Action, the Examiner alleges that Sasmazel '101 discloses that a storage partial unit in a transmitting terminal device includes a D-register containing a device identification signal, but (as mentioned above) Sasmazel '101 does not disclose a storage partial unit in a transmitting terminal device, and in fact it does not disclose a D-register in any storage partial unit. At page 8, lines 3-7 of the final Office Action, the Examiner cites paragraph 45 of Sasmazel '101, but that paragraph does not mention a storage partial unit or a D-register contained therein.

Furthermore, in making the above assertion, the Examiner cites column 11, lines 1-10 for the alleged disclosure of a request containing a terminal ID and an IP address code but those items are not found at column 11, lines 1-10 of Sasmazel '101.

Moreover, at page 3, lines 3-12 of the final Office Action, the Examiner alleges that Sasmazel '101 discloses a C-register storing a coding key and connected to a sender partial unit (citing Figure 1 of the reference). However, a review of Sasmazel '101 reveals that the memory for storing a coding key, as contained in call complex 102, is not connected to end unit 110, or to any sender partial unit contained therein.

In addition, at page 3, lines 13-16 of the final Office Action, the Examiner alleges that Sasmazel '101 discloses a storage partial unit of each transmitting terminal device which includes at least one temporary storage register for the temporary storage of coding keys of

other transmitting terminal devices, citing column 11, lines 20-30 of the reference. However, the end unit identification code referred to at column 11, lines 20-21 of Sasmazel '101 is not a key for encoding/decoding transmissions, but rather it is the identification code for end unit 2 as stored in end unit 2 itself. Moreover, it does not constitute a coding key of other end units or transmitting terminal devices as alleged by the Examiner.

At page 3, line 17-page 4, line 11 of the final Office Action, the Examiner refers to the call complex 102 as having an MD-register for storing a master decoding key, and also refers to the end units as having C-registers. However, none of the cited portions of Sasmazel '101 discloses or suggests C-registers or D-registers. This is admitted on page 5 of the Office Action (see page 5, lines 6-11 of the final Office Action).

In the latter regard, at page 5, lines 12-18 of the final Office Action, the Examiner cites Figures 3 and 5 of Zeidler '530 , and specifically the table 78 of Figure 5, as corresponding to the claimed C-register and D-register. However, the disclosure of Zeidler '530 does not support this allegation.

Specifically, Zeidler '530 does not disclose that the table 78 is part of a storage partial unit, as claimed. In addition, a review of the specification of Zeidler '530 fails to reveal a disclosure of all of the operations performed with respect to the C-register and the D-register, as recited in independent claim 5 of the present application. For example, Zeidler '530 does not disclose that C-registers of an information transmitting terminal device are provided with a master coding key collaborating with a master decoding key stored in an MD-register of a

central traffic coordinating unit, as recited in independent claim 5 of the present application. In the latter regard, no portions of the disclosure of Zeidler '530 are cited as disclosing the specifically recited operations relating to the C-register and the D-register of independent claim 5.

In addition, in the second complete paragraph on page 4 of the final Office Action, the Examiner alleges that, in the storage partial unit of a first transmitting terminal device, there is only information free from the coding key of the first transmitting terminal device, the Examiner citing column 8, lines 15-25 of Sasmazel '101. However, the cited portion of Sasmazel '101 merely discusses encryption, transmission of an authorization request, and identification of the request, but does not at all disclose or suggest that there is, in a storage partial unit of a first transmitting terminal device, only information free from the coding key of a first transmitting terminal device.

Furthermore, referring again to the second complete paragraph on page 4 of the final Office Action, there is no disclosure or suggestion of a temporary storage register of a first transmitting terminal device, and the end-unit-to-end-unit session key referred to at column 11, lines 35-45 of Sasmazel '101 (cited in the final Office Action) is not a coding key of a first transmitting terminal device, as alleged in the final Office Action.

In the third complete paragraph on page 4 of the final Office Action, the Examiner alleges that Sasmazel '101 discloses that only the coding key of the first transmitting terminal device (end unit) participating in an information exchange is temporarily stored in a

temporary storage register of a second transmitting terminal device, the Examiner again citing column 11, lines 35-45 of the reference. However, such a temporary storage register of a transmitting terminal device is not disclosed in the cited portion of Sasmazel '101, or in Sasmazel '101 in its entirety. Furthermore, the cited portion of Sasmazel '101 does not refer to a coding key of a first transmitting terminal device, but rather refers to an end unit to end unit session key EUEUSK. In fact, the lack of disclosure of any temporary storage register in Sasmazel '101 is admitted on page 5 of the final Office Action (specifically, see page 5, lines 6-11 of the final Office Action).

In the latter regard, at page 6, lines 1-4 of the final Office Action, the Examiner cites the active transaction table 81 of Figure 5 of Zeidler '530 as corresponding to the claimed temporary storage register of independent claim 5. However, Zeidler '530 does not disclose the specific functions of the temporary storage registers included in the storage partial unit, as recited in independent claim 5. In fact, no portion of the specification of Zeidler '530 is cited in the final Office Action as describing the functions of the active transaction table 81 of Figure 5 of Zeidler '530.

The operation of the active transaction table 81 of Figure 5 of Zeidler '530 is described at column 13, lines 42-45 of the reference, but it only describes an operation whereby a transaction trace number and a terminal identification number related to a transaction initiated by a terminal are stored, the transaction being a transmission requested by the terminal. In contrast, independent claim 5 of the present application calls for the

storage, in a temporary storage register of a first information transmitting terminal device, of the coding key of a second information transmitting terminal device which is participating in an information exchange with the first information transmitting terminal device.

For the reasons stated above, it is respectfully submitted that, contrary to the assertions in the final Office Action, Sasmazel '101 in view of Zeidler '530 does not disclose or suggest the invention as recited in independent claim 5. Therefore, a rejection under 35 U.S.C. 103 is inappropriate.

In addition, the dependent claims of the present application further distinguish the invention from the cited prior art. Specifically, referring to dependent claim 6, in paragraph 4 on page 6 of the final Office Action, it is alleged that Sasmazel '101 discloses temporary storage registers of transmitting terminal devices connected to a sender partial unit, citing Figures 1-3 of the reference. However, as indicated above, Sasmazel '101 does not disclose sender partial units of terminal devices, and therefore there is no disclosure or suggestion of temporary storage registers of transmitting terminal devices connected to a sender partial unit.

Additional Arguments

The main concept of the present invention is that the coding key and the decoding key cooperate with each other and with the information transmitting terminal devices, but the coding key is never stored and/or generated in or by its own information transmitting

terminal device. Rather, it is stored in the central traffic coordinating unit, as seen in Figure 1 of the present application. In addition, the coding key and the decoding key are never stored together in the same place. The decoding key is stored in its information transmitting terminal device from the outset, whereas the coding key is stored at the outset in the central traffic coordinating unit, but is sent from that location to another information transmitting terminal device which does not have the cooperating decoding key. Thus, the coding key/ decoding key pairs are never stored in the same place. This is an important distinction between the present invention and the prior art cited against this application.

Another major distinction between the present invention and the cited prior art resides in the fact that, in the invention, asymmetric keys are used, while the prior art arrangements use symmetric keys. That is, both references cited in the final Office Action use symmetric keys for communications — specifically, DES in Zeidler '530 and session keysin Sasmazel '101. The main problem with the use of symmetric keys (DES, AES, Blowfish, Triple ES, Serpent, Twofish etc.) is the vulnerability experienced when distributing these keys. This is quite obvious and is pointed out in Zeidler '530 as follows: "The security of any system based on DES processing is dependent upon the integrity of key generation and distribution as well as upon the human-related management and operational procedures established for the system" (quoting from column 3, lines 8-12 of Zeidler '530). Furthermore these keys need to be changed on a regular basis: "[M]aster keys are typically used for longer periods of time that could extend into many months" (quoting from column 3, lines 34-35 of Zeidler

'530). In-house attacks cannot be excluded, only lessened: "Therefore, the potential vulnerability to in-house sophisticated attacks is lessened" (quoting from column 5, lines 20-22 of Zeidler '530). Furthermore, in a system using symmetric keys, the keys needed to decrypt the information are present at several points in the network (see Acquirer and Network switch - retransmit the keys in Zeidler '530).

In contrast, in the present invention, solution keys needed to decrypt information are only present at the point where the information is intended to be used.

All the symmetric encoding solutions have well known attacks, such as: linear cryptanalysis (http://en.wikipedia.org/wiki/Linear_cryptanalysis), differential cryptoanalysis (see "Eli Biham and Adi Shamir in the late 1980s, who published a number of attacks against various block ciphers and hash functions, including a theoretical weakness in the Data Encryption Standard (DES)." -- http://en.wikipedia.org/wiki/Differential_cryptanalysis), impossible differential cryptoanalysis, integral cryptoanalysis (applied to Twofish by Stefan Lucks).

Thus, transmission of messages encrypted only with symmetric keys has several security issues. Accordingly, the present invention excludes transferring any information encrypted only with symmetric keys, and excludes sending any key that can be used to decrypt any information.

Confidentiality is a main attribute of any public key encryption. Confidentiality means ensuring that information is accessible only to those authorized to have access. Since the

present invention uses the very same mathematical base as the public key encryption, it provides confidentiality. Thus, in the invention, only the managing server has the encoding keys of the endpoints, and therefore only the server can contact them. Only the endpoints of a given network have the encoding key of the managing server, and therefore only the endpoints belonging to the network can initiate communication to the managing server.

All of the prior art systems and networks, including those disclosed in Sasmazel '101 and Zeidler '530, miss the main point of the present invention, that is, use of asymmetric encoding algorithm key pairs. Thus, the present invention provides the following features and advantages:

(1) any decoding key identifies an information target point (endpoint or server), and this decoding key never leaves this point;

(2) possessing any server encoding key belonging to a server decoding key embodies entitlement to access the aforementioned server's network (the server itself and the other endpoints), and these keys are never transmitted through the network;

(3) on the server side, possessing any endpoint's encoding key embodies entitlement to manage the endpoint, provided that the endpoint has the server's encoding key;

(4) keys needed to encrypt any useful information are only present at the point where information is intended to be utilized, and these keys are never transmitted throughout the network;

(5) in-house attacks are excluded since the server never retransmits any useful information (only encrypted keys); and

(6) operators of the system have no ability to eavesdrop on the communication while, in contrast, Zeidler '530 provides that the operator of an acquirer or network switch can access all information, and Sesmazel '101 provides that the operator of the call complex can access all information on both sides.

Conclusion

In the view of the above, it is submitted that the claims of the present application are in condition for allowance, and early issuance of this application is solicited. If there are any problems or issues remaining, the Examiner is requested to telephone the undersigned attorney at the below-listed local telephone number.

A Petition for Extension of Time and a Request for Continued Examination (RCE) are being filed concurrently herewith, and contain an authorization to charge the extension and RCE fees to Deposit Account 19-1070. The Commisioner is authorized to charge any

other fees which are incurred to Deposit Account No. 19-1070. A duplicate of this sheet is enclosed.

Respectfully submitted,
Miklós JOBBÁGY et al

By: _____
Joseph G. Seeber
Reg. No. 27,719

Post Office Box 750
Great Falls, VA 22066
Telephone: (703)430-1702
Facsimile: (703)450-7914

other fees which are incurred to Deposit Account No. 19-1070. A duplicate of this sheet is enclosed.

Respectfully submitted,
Miklós JOBBÁGY et al

By: _____
Joseph G. Seeber
Reg. No. 27,719

Post Office Box 750
Great Falls, VA 22066
Telephone: (703)430-1702
Facsimile: (703)450-7914

COPY